9111-14

DEPARTMENT OF HOMELAND SECURITY

6 CFR Part 5

[Docket No. DHS-2018-0064]

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-024 CBP Intelligence Records System (CIRS) System of Records

AGENCY: Department of Homeland Security.

ACTION: Final rule.

SUMMARY: The Department of Homeland Security is issuing a final rule to amend its regulations to exempt portions of a newly established system of records titled, "DHS/CBP-024 CBP Intelligence Records System (CIRS) System of Records" from certain provisions of the Privacy Act. Specifically, the Department exempts portions of the "DHS/CBP-024 CBP Intelligence Records System (CIRS) System of Records" from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: This final rule is effective **[INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number DHS-2018-0064, at:

- Federal eRulemaking Portal: http://www.regulations.gov. Please follow the instructions for submitting comments.

- Mail and hand delivery on commercial delivery: U.S. Customs and Border Protection, Privacy and Diversity Office, ATTN: Privacy Officer – Debra L. Danisek, 1300 Pennsylvania Ave., NW, Washington, D.C. 20229.

Instructions: All submissions received must include the agency name and docket number for this rule. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For privacy issues please contact: Chief Privacy Officer, Privacy Office Philip S. Kaplan at 202-343-1717.

SUPPLEMENTARY INFORMATION:

I. Background:

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) published a notice of proposed rulemaking in the *Federal Register* (82 FR 44124, September 21, 2017) proposing to exempt portions of this system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. DHS issued the "DHS/CBP-024 CBP Intelligence Records System (CIRS) System of Records" in the *Federal Register* at 82 FR 44198, on September 21, 2017, to provide notice to the public that DHS/CBP collects and maintains records generated, received, or collected by the CBP Office of Intelligence, or other offices within CBP that support the law enforcement intelligence mission, that is analyzed and disseminated to CBP executive management and operational units for law enforcement, intelligence,

counterterrorism, and other homeland security purposes. CIRS contains data from a variety of sources within and outside of CBP to support law enforcement activities and investigations of violations of U.S. laws, administration of immigration laws and other laws administered or enforced by CBP, and production of CBP law enforcement intelligence products. CIRS is the exclusive CBP SORN for finished intelligence products and any raw intelligence information, public source information, or other information collected by CBP for an intelligence purpose that is not covered by an existing DHS SORN. CIRS records were previously covered by DHS/CBP-006 - Automated Targeting System SORN (77 FR 30297, May 22, 2012) and DHS/CBP-017 - Analytical Framework for Intelligence SORN (77 FR 13813, June 7, 2012).

DHS/CBP invited comments on both the Notice of Proposed Rulemaking (NPRM) and System of Records Notice (SORN).

II. Public Comments:

DHS received thirty-two comments on the CBP CIRS NPRM and four on the CBP CIRS SORN. Of the thirty-six total comments, thirteen were erroneously filed relating to the republication of the DHS Alien File, Index, and National File Tracking system (A-File). DHS will not respond to comments regarding the publication of the A-File SORN in this Final Rule. Of the remaining substantive comments for CIRS: (1) seventeen related to transparency; (2) two related to the collection of information not specifically relevant to an investigation; and (3) four were duplicates of two formal briefs submitted for both the SORN and the NPRM. The following is an analysis of the substantive comments and questions submitted by the public.

Comment: DHS should not hide what it is collecting by exempting the information from Privacy Act protections.

Response: DHS published the CIRS SORN in compliance with the notification requirements of the Privacy Act, subsection 552a(e)(4), and thus, is being transparent of its collection activities. The CIRS SORN describes the information that DHS collects and retains in association with this system of records. DHS does not seek to hide this collection or exempt it from the notification requirements of the Privacy Act; rather, it seeks exemptions to ensure that records critical to law enforcement and intelligence activities need not be shared in the event that such sharing might jeopardize the investigation or otherwise compromise DHS operations.

Comment: DHS's collection of records in CIRS is overly broad because, as stated in the NPRM, DHS may be collecting information that "may not be strictly relevant or necessary to a specific investigation."

Response: In order to conduct a complete investigation, it is necessary for DHS/CBP to collect and review large amounts of data in order to identify and understand relationships between individuals, entities, threats and events, and to monitor patterns of activity over extended periods of time that may be indicative of criminal, terrorist, or other threat.

Comment: The SORN contains materially false claims concerning the status of the rulemaking for Privacy Act exemptions that are directly contradicted by the Notice of Proposed Rulemaking for those exemptions.

Response: The Secretary of Homeland Security issued a proper NPRM, pursuant to the Privacy Act, the Federal Register, and Office of Management and Budget (OMB)

requirements, received comments from the public as part of the notice and comment procedures of the Administrative Procedure Act, and is issuing this final rule in conformance with those requirements.

Comment: Proposed routine uses would circumvent Privacy Act safeguards and contravene legislative intent.

Response: DHS's collection of records in CIRS is intended to permit DHS/CBP to review large amounts of data in order to identify and understand relationships between individuals, entities, threats and events, and to monitor patterns of activity over extended periods of time that may be indicative of criminal, terrorist, or other threat. The SORN is consistent with the legislative intent of the Privacy Act to ensure fair practices, collection, and uses of individuals' personal information. The routine uses, as written in the CIRS SORN, and disclosures of such records, are compatible with the purpose for which they are originally collected and used by DHS/CBP.

After consideration and review of the public comments, DHS has determined that the exemptions should remain in place, and will implement the rulemaking as proposed.

List of Subjects in 6 CFR Part 5

Freedom of information, Privacy.

For the reasons stated in the preamble, DHS amends Chapter I of Title 6, Code of Federal Regulations, as follows:

PART 5--DISCLOSURE OF RECORDS AND INFORMATION

1. The authority citation for part 5 continues to read as follows:

Authority: 6 U.S.C. 101 et seq.; Pub. L. 107-296, 116 Stat. 2135; 5 U.S.C. 301. Subpart A also issued under 5 U.S.C. 552. Subpart B also issued under 5 U.S.C. 552a.

2. Add paragraph 79 to appendix C to part 5 to read as follows:

Appendix C to Part 5 – DHS Systems of Records Exempt From the Privacy Act

* * * * *

79. The DHS/CBP-024 CBP Intelligence Records System (CIRS) System of Records consists of electronic and paper records and will be used by DHS and its components. The CIRS is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. The CIRS contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I); (e)(5), and (e)(8); (f); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(1) and (k)(2), has exempted this system from the following provisions of the Privacy Act, 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f). When this system receives a record from another system exempted in that source system under 5 U.S.C. 552a(k)(1), (k)(2), or (j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set

forth here. Exemptions from these particular subsections are justified, on a case by case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process. Information on a completed investigation may be withheld and exempt from disclosure if the fact that an investigation occurred remains sensitive after completion.

(b) From subsection (d) (Access and Amendment to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In

addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules) because portions of this system are exempt from the individual access and amendment provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access, amend, and view records pertaining to themselves in the

system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore, DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's refusal to amend a record, refusal to comply with a request for access to records, failure to maintain accurate, relevant timely and complete records, or its failure to otherwise comply with an individual's right to access or amend records.

Philip S. Kaplan,
Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2018-27944 Filed: 12/26/2018 8:45 am; Publication Date: 12/27/2018]